AMENDED IN SENATE AUGUST 22, 2014

AMENDED IN SENATE AUGUST 4, 2014

AMENDED IN SENATE JUNE 12, 2014

AMENDED IN ASSEMBLY MAY 23, 2014

CALIFORNIA LEGISLATURE—2013–14 REGULAR SESSION

ASSEMBLY BILL No. 2200

Introduced by Assembly Member John A. Pérez

February 20, 2014

An act to add and repeal Article 3.9 (commencing with Section 8574.50) of Chapter 7 of Division 1 of Title 2 of the Government Code, relating to cyber security.

LEGISLATIVE COUNSEL'S DIGEST

AB 2200, as amended, John A. Pérez. California Cyber ~~Security Commission.~~ *Security.*

Existing law establishes various advisory boards and commissions in state government with specified duties and responsibilities. Existing law establishes in state government the Governor's office of Emergency Services *and the Department of Technology*.

~~This bill would create the California Cyber Security Commission in the Governor's Office of Emergency Services, consisting of 15 members comprised of representatives from state government, appointed representatives from the technology or cybersecurity industry and the utility or energy industry, and an appointed representative of California's critical infrastructure interests. The bill would also authorize the commission to appoint representatives from state, local, federal, and private entities to form an advisory board in order to receive input or~~

~~advice concerning the implementation of the duties of the commission. The duties of the commission would include establishing cyber-attack response strategies and performing risk assessments on state information technology systems. The bill would require the commission to meet on a quarterly basis, or as specified, and would allow the commission to issue a report to the Governor's Office and the Legislature that details the activities of the commission and makes recommendations to improve California's cybersecurity preparedness.~~

This bill would continue in existence the California Cyber Security Task Force, previously created by the Governor's Office of Emergency Services and the Department of Technology, in the Governor's Office of Emergency Services. This bill would require the office and the department to convene stakeholders to act in an advisory capacity and compile policy recommendations on cyber security for the state. The bill would require the task force to meet quarterly, or more often as necessitated by emergency circumstances. This bill would require the task force to complete and issue a report of policy recommendations to the Governor's office and the Legislature by January 1, 2015.

This bill would create the California Cyber Security Steering Committee in the Governor's Office of Emergency Services, consisting of 13 members comprised of representatives from state government, and appointed representatives with specific expertise or from the technology or cybersecurity industry and the utility or energy industry. This bill would require the steering committee to seek to implement the policy recommendations of the task force based on specified priorities. This bill would require the office and the department to collaborate with the steering committee.

This bill would authorize the Governor's Office of Emergency Services and the Department of Technology to conduct the strategic direction of risk assessments performed by the Military Department's Computer Network Defense Team.

The bill would abolish the ~~commission~~ *California Cyber Security Task Force and the California Cyber Security Steering Committee*, and repeal these provisions, on January 1, ~~2019~~ *2020*.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Article 3.9 (commencing with Section 8574.50) is added to Chapter 7 of Division 1 of Title 2 of the Government Code, to read:

Article 3.9. California Cyber Security ~~Commission~~

8574.50. The Legislature finds and declares all of the following:

(a) The State of California's growing dependence on technology has made it increasingly vulnerable to both foreign and domestic cyber security attacks. Thus far, there has been a fragmented approach to this issue with independent efforts occurring through federal, state, and local government, as well as in the state's universities and within private industry. For the purposes of public safety and protection of public assets, the state has a role in coordinating and improving its overall security and response capabilities.

(b) The market for cyber security is estimated to be more than seventy billion dollars ($70,000,000,000) in 2014. Of that amount, sixty-seven billion dollars ($67,000,000,000) is estimated to be spent nationally by private companies for computer and network security and the United States Department of Defense is planning to spend four billion six hundred million dollars ($4,600,000,000). The United States Department of Defense is planning on spending twenty-three billion dollars ($23,000,000,000) over the next five years. Overall spending is expected to increase rapidly as recognition of threats becomes more ubiquitous. The California economy stands to greatly benefit from this industry growth.

(c) The State of California has already made investments for the purpose of cyber security; examples of which are research funding for the Lawrence Livermore National Laboratory and funding to augment a cyber security assessment and response team within the California National Guard.

(d) The California Cyber Security Task Force was initiated in May 2013 for the purposes of identifying critical threats, assembling primary stakeholders, and highlighting the growing importance of the issue. Among other things, this has increased awareness of the state's compliance with the new federal National Institute of Standards and Technology (NIST) standards and the

Office of Emergency Services establishing Emergency Function 18, created particularly for cyber security.

(e) Over 50,000 new malicious online activities are identified every day, according to the United States Department of Defense. Incidents of sophisticated and well-coordinated attacks and data breaches are occurring more regularly, the average cost of which amounts to more than ten million dollars ($10,000,000). In 2012, a data breach to the state of South Carolina required more than twenty million dollars ($20,000,000) in response and restitution. The State of California is vulnerable technically, legally, and financially to these threats.

(f) The State of California recognizes that cyber security is both a current and future state security issue that requires a whole-of-government policy solution, not just a technology one. The State of California intends to demonstrate leadership on the issue in conjunction with federal and local governments.

(g) The State of California intends to balance cyber security interests of its citizens and public assets with transparency and protection of privacy rights.

8574.51. (a) There is hereby continued in existence the California Cyber Security Task Force, created in 2013 by the Governor's Office of Emergency Services and the Department of Technology, in the Governor's Office of Emergency Services.

(b) The Governor's Office of Emergency Services and the Department of Technology shall convene stakeholders, both public and private, to act in an advisory capacity and compile policy recommendations on cyber security for the State of California. The California Cyber Security Task Force shall complete and issue a report of policy recommendations to the Governor's office and the Legislature. The report shall be completed in compliance with Section 9795.

(c) The California Cyber Security Task Force shall meet quarterly, or more often as necessitated by emergency circumstances, within existing resources to ensure that the policy recommendations from the report are implemented and any necessary modifications which may arise are addressed in a timely manner.

(d) The Governor's Office of Emergency Services and the Department of Technology shall collaborate with the Cyber Security Steering Committee created pursuant to Section 8574.52

to use their combined expertise to streamline the implementation of policy recommendations set forth in the California Cyber Security Task Force's report. This collaboration shall be guided by the priorities set forth in Section 8574.54 and shall timely realize the state's cyber security goals.

(e) The Governor's Office of Emergency Services and the Department of Technology shall be authorized to conduct the strategic direction of risk assessments performed by the Military Department's Computer Network Defense Team as budgeted in Item 8940-001-0001 of the Budget Act of 2014.

~~8574.51.~~

8574.52. (a) There is in the Governor's Office of Emergency Services the~~ California~~ Cyber Security~~ Commission. The commission~~ *Steering Committee, which* shall consist of the following members:

(1) The Director of Emergency Services, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Office of Emergency Services' information technology and information security duties.

~~(2) The Chief of the Office of Information Security, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the chief's information technology and information security duties set forth in Chapter 5.7 (commencing with Section 11549) of Part 1 of Division 3.~~

(2) The Director of the Department of Technology, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the director's information technology and information security duties set forth in Chapter 5.6 (commencing with Section 11545).

(3) The Attorney General, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Department of Justice's information technology and information security.

(4) The Adjutant General of the Military Department, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Military Department's information technology and information security.

~~(5) The Insurance Commissioner, or his or her designee with knowledge, expertise, and decisionmaking authority with respect~~

~~to the Department of Insurance's information technology and information security.~~

~~(6)~~

(5) The Secretary of Health and Human Services, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the California Health and Human Services Agency's information technology and information security.

~~(7)~~

(6) The Secretary of the California Transportation Agency, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the agency's information technology and information security.

~~(8) The Controller, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the office of the Controller's information technology and information security.~~

~~(9)~~

(7) The Commissioner of the California Highway Patrol, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the California Highway Patrol's information technology and information security.

~~(10)~~

(8) The Commander of the State Threat Assessment Center, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the State Threat Assessment Center's information technology and information security.

~~(11)~~

(9) A representative ~~from the private sector in the technology or cybersecurity industry~~ *with cybersecurity expertise*, who shall be appointed by the Governor.

~~(12)~~

(10) A representative of the state's higher education system with knowledge, expertise, and decisionmaking authority with respect to information technology and information security, who shall be appointed by the Governor.

~~(13)~~

(11) A representative of the Public Utilities Commission *or*, California Energy ~~Commission, or California Independent System Operator~~ *Commission* with knowledge, expertise, and

decisionmaking authority with respect to information technology and information security, who shall be appointed by the Governor.

~~(14)~~

(12) A representative from the ~~utility or energy industry~~ *private sector in the technology or cybersecurity industry*, who shall be appointed by the Speaker of the Assembly.

~~(15)~~

(13) A representative ~~of California's critical infrastructure interests, such as air traffic control, ports, and water systems~~ *from the utility or energy industry*, who shall be appointed by the Senate Committee on Rules.

(b) (1) Each representative appointed by the Governor, Speaker of the Assembly, or Senate Committee on Rules shall be appointed to serve a two-year term.

(2) Any representative may serve consecutive terms.

(c) Any designee shall serve at the pleasure of the official who designated them.

(d) Eight members shall constitute a quorum for the transaction of business, and all official acts of the ~~commission~~ *steering committee* shall require the affirmative vote of a majority of its members constituting a quorum.

(e) The members of the ~~commission~~ *steering committee* shall serve without compensation, except that each member of the ~~commission~~ *steering committee* shall be entitled to receive his or her actual necessary traveling expenses while on official business of the ~~commission~~ *steering committee*.

~~8574.52. (a) The commission may appoint representatives to form an advisory board in order to receive input or advice concerning the implementation of the duties of the commission. The commission may expand, as needed, the advisory board to accommodate the representation necessary to inform and advance the duties of the commission.~~

~~(b) The advisory board may be comprised of one or more representatives from the following:~~

~~(1) The United States Department of Homeland Security.~~

~~(2) The National Institute for Standards and Technology.~~

~~(3) State government.~~

~~(4) Local government.~~

~~(5) California's utility grid, both private and public.~~

~~(6) Technology firms, cybersecurity firms, critical infrastructure operators, utility providers, financial firms, health care providers, and other private industries.~~

~~(7) California's cybersecurity law enforcement apparatus, which includes:~~

~~(A) The Attorney General's eCrimes Unit.~~

~~(B) The five regional task forces of the High Technology Theft Apprehension and Prosecution Program.~~

~~(C) The Department of the California Highway Patrol.~~

~~(8) Entities operating with the commission to perform its duties, including:~~

~~(A) The State Threat Assessment Center and fusion centers, for the purpose of sharing information that informs preventive actions.~~

~~(B) The California National Guard's Computer Network Defense Team, for the purpose of coordinating comprehensive risk assessments.~~

~~(C) California's public and private universities and laboratories for the purpose of directing research and best utilizing its results.~~

~~(c) The commission shall appoint each representative by a majority vote of its members constituting a quorum. Each representative shall serve at the pleasure of the commission.~~

~~8574.53. The commission shall meet quarterly, or more often as determined by a majority vote of its members constituting a quorum, or in the event of an emergency.~~

8574.54. The ~~duties of the commission shall include the following:~~ *Cyber Security Steering Committee shall seek to implement the policy recommendations of the California Cyber Security Task Force based on the following priorities:*

(a) Developing within state government cyber prevention, defense, and response strategies and defining a hierarchy of command within the state for this purpose. This duty includes, but is not limited to, the following activities:

(1) Performing comprehensive risk assessments on state information technology systems. The ~~Chief Information Security Officer shall coordinate the process of performing risk assessments and the~~ assessments shall be performed by such entities as the California National Guard's Computer Defense Network Team and the State Threat Assessment Center, ~~in addition to~~ *with guidance and assistance from* other public and private sector entities.

(2) ~~Creating~~ *Using assessment results and other state-level data to create* a risk profile of public assets, critical infrastructure, public networks, and private operations susceptible to cyber attacks. *The risk profile shall include the development of statewide contingency plans including, but not limited to, Emergency Function 18 of the State Emergency Plan.*

~~(3) Coordinating efforts to reduce state information technology risks and gaps in existing service.~~

(b) Partnering with the United States Department of Homeland Security to develop an appropriate information sharing system that allows for a controlled and secure process to effectively disseminate cyber threat and response information and data to relevant private and public sector entities. This information sharing system shall reflect state priorities and target identified threat and capability gaps.

(c) Providing recommendations for information technology security standards for all state agencies using, among other things, protocols established by the National Institute for Standards and Technology and reflective of appropriate state priorities.

(d) Compiling and integrating, as appropriate, the research conducted by academic institutions, federal laboratories, and other cybersecurity experts into state operations and functions.

(e) Expanding the state's public-private cybersecurity partnership network both domestically and internationally to assist in the state's efforts to prevent and respond to cyber threats and cyber attacks as well as enhance overall cyber detection capability.

(f) Developing and providing ~~a~~ training ~~program~~ *programs with the state's higher education and labor entities* to produce a credentialed and qualified state cybersecurity workforce. This program should include training based on the requirements and protocols outlined in models such as Department of Defense Directive 8570. ~~The commission shall work with state workforce and labor entities as well as the state's higher education systems, federal agencies, and others to provide training and develop curriculum.~~

~~(g) Analyzing, in conjunction with the Department of Insurance, the development of a strategy to acquire and incorporate cyber insurance into the procurement and administrative processes of state agencies to protect state assets and information.~~

~~(h)~~

(g) Expanding collaboration with the state's law enforcement apparatus assigned jurisdiction to prevent, deter, investigate, and prosecute cyber attacks and information technology crime, including collaboration with entities like the High-Tech Theft Apprehension Program, and its five regional task forces, the Department of the California Highway Patrol, and the Attorney General's eCrimes unit. Collaboration will include information sharing that will enhance their capabilities including assistance to better align their activities with federal and local resources, provide additional resources, and extend their efforts into regions of the state not currently represented.

~~(i)~~

(h) Proposing, where appropriate, potential operational or functional enhancement to the state's cybersecurity assessment and response capabilities, as well as investment or spending recommendation and guidance for the state's information technology budget and procurement.

~~(j)~~

(i) Coordinating the pursuit of fiscal resources including federal grants and other funding opportunities to enhance the state's cybersecurity, information technology, data privacy, cyber research, and technology-based emergency response capabilities.

8574.55. The ~~commission~~ *California Cyber Security Task Force* shall take all necessary steps to protect personal information, public and private sector data, as well as ensure consumer privacy, when implementing its duties.

8574.56. (a) The ~~commission~~ *California Cyber Security Task Force* may issue ~~a report~~ *reports, in addition to the report described in subdivision (b) of Section 8574.51,* to the Governor's office and the Legislature detailing the activities of the ~~commission~~ *task force*, including, but not limited to, progress on the ~~commission's~~ *California Cyber Security Task Force's* various tasks and actions taken and recommended in response to an incident, as appropriate.

(b) The reports shall be submitted in compliance with Section 9795.

8574.57. The ~~commission~~ *California Cyber Security Task Force* may engage or accept the services of agency or department personnel, accept the services of stakeholder organizations, and accept federal, private, or other nonstate funding, to operate,

manage, or conduct the business of the ~~commission~~ *California Cyber Security Task Force*.

8574.58. The ~~commission~~ *California Cyber Security Task Force* shall operate within the current information technology budget of each department and agency they serve. Each department and agency shall cooperate with the commission and furnish it with information and assistance that is necessary or useful to further the purposes of this article.

8574.59. This article shall become inoperative on January 1, ~~2019~~*, 2020,* and shall be repealed as of that date.

O